IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

TQP DEVELOPMENT, LLC, ***Plaintiff***, **v.** **1. 1-800-FLOWERS.COM, INC.** **2. AMWAY CORP.;** **3. ALTICOR INC.;** **4. CELLCO PARTNERSHIP;** **5. HSN, INC.;** **6. MICRO ELECTRONICS, INC.;** **7. NEWEGG INC.;** **8. QVC, INC.;** **9. SPRINT NEXTEL CORPORATION; and** **10. VERIZON COMMUNICATIONS, INC.** ***Defendants***,	**Civil Action No.** **JURY TRIAL DEMANDED**

ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which TQP Development, LLC ("TQP") makes the following allegations against 1-800-Flowers.com, Inc.; Amway Corp.; Alticor Inc.; Cellco Partnership; HSN, Inc.; Micro Electronics, Inc.; Newegg Inc.; QVC, Inc.; Sprint Nextel Corporation and Verizon Communications, Inc. (collectively, "Defendants"):

PARTIES

1. Plaintiff TQP Development, LLC is a Texas limited liability company having a principal place of business of 207C North Washington Street, Marshall, Texas 75670.

2. On information and belief, Defendant 1-800-Flowers.com, Inc. ("1-800-Flowers") is a Delaware corporation with its principal place of business at 1 Old Country Rd., Suite 500, Carle Place, NY 11514. 1-800-Flowers has appointed The Corporation

Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

3. On information and belief, Defendant Alticor, Inc. ("Alticor") is a Michigan corporation with its principal place of business at 7575 Fulton Street East, Ada, MI 49355. Alticor, Inc. has appointed The Corporation Company, 30600 Telegraph Rd., Bingham Farms, MI 48025 as its agent for service of process.

4. On information and belief, Defendant Amway Corp. ("Amway") is a Virginia corporation with its principal place of business at 7575 Fulton Street East, Ada, MI 49355. Amway has appointed CT Corporation System 4701 Cox Rd. Suite 301, Glen Allen, VA 23060 as its agent for service of process.

5. On information and belief, Defendant Cellco Partnership ("Cellco") is a Delaware General Partnership with its principal place of business at One Verizon Way, Basking Ridge, NJ 07920. Cellco has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

6. On information and belief, Defendant HSN, Inc. ("HSN") is a Delaware corporation with its principal place of business at 1 HSN Dr., Saint Petersburg, FL 33729. HSN has appointed Corporation Service Company 2711 Centerville Rd., Suite 400, Wilmington, DE as its agent for service of process.

7. On information and belief, Defendant Micro Electronics, Inc. ("Micro Electronics") is a Delaware corporation with its principal place of business at 4119 Leap Rd., Hilliard, OH 43026. 1-800-Flowers has appointed Registered Agents, Ltd. 1220 N. Market St., Suite 804, Wilmington, DE 19801 as its agent for service of process.

8. On information and belief, Defendant Newegg, Inc. ("Newegg") is a Delaware corporation with its principal place of business at 16839 Gale Ave., City of Industry, CA 91745. Newegg has appointed Corporation Service Company 2711 Centerville Rd., Suite 400, Wilmington, DE as its agent for service of process.

9. On information and belief, Defendant QVC, Inc. ("QVC") is a Delaware corporation with its principal place of business at 1200 Wilson Dr., West Chester, PA 19380. QVC has appointed Corporation Service Company 2711 Centerville Rd., Suite 400, Wilmington, DE as its agent for service of process.

10. On information and belief, Defendant Sprint Nextel Corporation ("Sprint") is a Kansas corporation with its principal place of business at 6200 Sprint Parkway, Overland Park, KS 66251. Sprint has appointed Corporation Service Company 200 SW 30th St., Topeka, KS 66611 as its agent for service of process.

11. On information and belief, Defendant Verizon Communications, Inc. ("Verizon") is a Delaware corporation with its principal place of business at One Verizon Way, Basking Ridge, NJ 07920. Verizon has appointed The Corporation Trust Company 1209 Orange St., Wilmington, DE 19801 as its agent for service of process.

JURISDICATION AND VENUE

12. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

13. Venue is proper in this district under 28 U.S.C. §§ 1391(c) and 1400(b). On information and belief, each Defendant has transacted business in this district, and has committed and/or induced acts of patent infringement in this district.

14. On information and belief, Defendants are subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statue, due at least to their substantial business in this forum, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct, and/or deriving substantial revenue from goods and services provided to individuals in Texas and in this Judicial District.

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 5,412,730

15. Plaintiff is the owner by assignment of United States Patent No. 5,412,730 ("the '730 Patent") entitled "Encrypted Data Transmission System Employing Means for Randomly Altering the Encryption Keys." The '730 Patent issued on May 2, 1995. A true and correct copy of the '730 Patent is attached as Exhibit A

16. Upon information and belief, Defendant 1-800-Flowers has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various 1-800-Flowers websites (including, without limitation to, ww10.1800flowers.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when 1-800-Flowers and/or 1-800-Flowers's customers connect to 1-800-Flowers's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server

to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of 1-800-Flowers's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. 1-800-Flowers provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. 1-800-Flowers generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. 1-800-Flowers encrypts data for transmission from the host server to the client. In addition, 1-800-Flowers directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. 1-800-Flowers generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. 1-800-Flowers decrypts data sent

from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant 1-800-Flowers is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant 1-800-Flowers is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant 1-800-Flowers is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

17. Upon information and belief, Defendant Alticor has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Alticor websites (including, without limitation to, www.amway.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Alticor and/or Alticor's customers connect to Alticor's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Alticor's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Alticor provides,

or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Alticor generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Alticor encrypts data for transmission from the host server to the client. In addition, Alticor directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Alticor generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Alticor decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Alticor is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Alticor is directly

infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Alticor is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

18. Upon information and belief, Defendant Amway has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Amway websites (including, without limitation to, www.amway.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Amway and/or Amway's customers connect to Amway's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Amway's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Amway provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Amway generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or

client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Amway encrypts data for transmission from the host server to the client. In addition, Amway directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Amway generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Amway decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Amway is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Amway is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Amway is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

19. Upon information and belief, Defendant Cellco has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in

the United States, by, among other things, methods practiced on various Cellco websites (including, without limitation to, www.verizon.net and myaccount.verizonwireless.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Cellco and/or Cellco's customers connect to Cellco's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Cellco's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Cellco provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Cellco generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Cellco encrypts data for transmission from the host server to the client. In addition, Cellco directs the client computer to encrypt data comprising information sent from the client to the host

server before it is transmitted over the link. Cellco generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Cellco decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Cellco is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Cellco is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Cellco is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

20. Upon information and belief, Defendant HSN has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various HSN websites (including, without limitation to, www.hsn.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when HSN and/or HSN's customers connect to HSN's website, a communication link is established between host

servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of HSN's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. HSN provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. HSN generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. HSN encrypts data for transmission from the host server to the client. In addition, HSN directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. HSN generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric

algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. HSN decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant HSN is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant HSN is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant HSN is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

21. Upon information and belief, Defendant Micro Electronics has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Micro Electronics websites (including, without limitation to, www.microcenter.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Micro Electronics and/or Micro Electronics' customers connect to Micro Electronics' website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Micro Electronics' website,

client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Micro Electronics provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Micro Electronics generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Micro Electronics encrypts data for transmission from the host server to the client. In addition, Micro Electronics directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Micro Electronics generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Micro Electronics decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a

useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Micro Electronics is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Micro Electronics is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Micro Electronics is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

22. Upon information and belief, Defendant Newegg has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Newegg websites (including, without limitation to, secure.newegg.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Newegg and/or Newegg's customers connect to Newegg's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Newegg's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Newegg provides, or directs the client computer to provide, a seed value for

both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Newegg generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Newegg encrypts data for transmission from the host server to the client. In addition, Newegg directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Newegg generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Newegg decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Newegg is directly infringing the ‘730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Newegg is directly infringing, literally infringing, and/or infringing the ‘730 Patent under

the doctrine of equivalents. Defendant Newegg is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

23. Upon information and belief, Defendant QVC has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various QVC websites (including, without limitation to, quality-s.qvc.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when QVC and/or QVC's customers connect to QVC's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of QVC's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. QVC provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. QVC generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced

at a time dependent upon a predetermined characteristic of the data being transmitted over said link. QVC encrypts data for transmission from the host server to the client. In addition, QVC directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. QVC generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. QVC decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant QVC is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant QVC is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant QVC is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

24. Upon information and belief, Defendant Sprint has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Sprint websites (including, without limitation to, www.myaccount.sprint.com) for transmitting data

comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Sprint and/or Sprint's customers connect to Sprint's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Sprint's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Sprint provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Sprint generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Sprint encrypts data for transmission from the host server to the client. In addition, Sprint directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Sprint generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data,

based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being produced each time a predetermined number of said blocks are transmitted over said link. Sprint decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Sprint is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Sprint is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Sprint is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

25. Upon information and belief, Defendant Verizon has been and now is infringing the '730 Patent in the State of Texas, in this judicial district, and elsewhere in the United States, by, among other things, methods practiced on various Verizon websites (including, without limitation to, www.verizon.net and myaccount.verizonwireless.com) for transmitting data comprising a sequence of blocks in encrypted form over a communication link covered by one or more claims of the '730 Patent to the injury of TQP. For example, when Verizon and/or Verizon's customers connect to Verizon's website, a communication link is established between host servers and the client computer. Data transmitted over this communication link comprises a sequence of

blocks, and is transmitted as packets in a sequence over the communication link. Certain data transmissions (both from the client computer to the host server, and from the host server to the client computer) are encrypted according to the claimed method. In order to communicate with encrypted portions of Verizon's website, client computers must agree to an encryption algorithm or protocol. Once that protocol is established by the host server, the client computer automatically implements the claimed encryption algorithm under the direction of the host server. Verizon provides, or directs the client computer to provide, a seed value for both the transmitter and receiver in a symmetric encryption algorithm, and uses the same key to encrypt and decrypt data. Verizon generates, or directs the client computer to generate, a first sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at the transmitter (whichever of the host server or client computer is sending the encrypted information), each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link. Verizon encrypts data for transmission from the host server to the client. In addition, Verizon directs the client computer to encrypt data comprising information sent from the client to the host server before it is transmitted over the link. Verizon generates, or directs the client computer to generate, a second sequence of pseudo-random key values, such as alpha and/or numerical values used to encrypt data, based on said seed value at said transmitter, each new key value in said sequence being produced at a time dependent upon a predetermined characteristic of the data being transmitted over said link such that said first and second sequences are identical to one another, as is used in a symmetric algorithm, a new one of said key values in said first and second sequences being

produced each time a predetermined number of said blocks are transmitted over said link. Verizon decrypts data sent from the client in order to use the data, and directs the client computer to decrypt data transmitted from the host server in order to provide a useable display to, for example, a user of the client computer. By virtue of performing each step of the claimed method, Defendant Verizon is directly infringing the '730 Patent. In addition, by virtue of performing some steps and directing and/or controlling others to perform the remaining steps, Defendant Verizon is directly infringing, literally infringing, and/or infringing the '730 Patent under the doctrine of equivalents. Defendant Verizon is thus liable for infringement of the '730 Patent pursuant to 35 U.S.C. § 271.

26. On information and belief, to the extent any marking was required by 35 U.S.C. §287, all predecessors in interest to the '730 Patent complied with any such requirements.

27. To the extent that facts learned in discovery show that Defendants' infringement of the '730 Patent is, or has been willful, Plaintiff reserves the right to request such a finding at the time of trial.

28. As a result of these Defendants' infringement of the '730 Patent, Plaintiff has suffered monetary damages and is entitled to a money judgment in an amount adequate to compensate for Defendants' infringement, but in no event less than a reasonable royalty for the use made of the invention by Defendants, together with interest and costs as fixed by the court, and Plaintiff will continue to suffer damages in the future unless Defendants' infringing activities are enjoined by this Court.

29. Unless a permanent injunction is issued enjoining these Defendants and their agents, servants, employees, representatives, affiliates, and all others acting on in

active concert therewith from infringing the '730 Patent, Plaintiff will be greatly and irreparably harmed.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendants have infringed, directly, jointly and/or indirectly, by way of inducing and/or contributing to the infringement of the '730 Patent, and that such infringement was willful;

2. A permanent injunction enjoining Defendants and their officers, directors, agents, servants, affiliates, employees, divisions, branches, subsidiaries, parents, and all others acting in active concert therewith from infringement, inducing the infringement of, or contributing to the infringement of the '730 Patent;

3. A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, and prejudgment and post-judgment interest for Defendants' infringement of the '730 Patent as provided under 35 U.S.C. § 284;

4. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees; and

5. Any and all other relief, at law or equity, to which Plaintiff may show itself to be entitled.

DEMAND FOR JURY TRIAL

Relator, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: May 6, 2011

Respectfully submitted,

By: *\s\ Andrew W. Spangler*
Andrew Wesley Spangler

Spangler Law PC
208 N. Green St., Suite 300
Longview, TX 75601
903-753-9300
Fax: 903-553-0403
Email: spangler@spanglerlawpc.com

Marc Fenster
mfenster@raklaw.com
Andrew D Weiss
Email: aweiss@raklaw.com
Adam Hoffman
Email: ahoffman@raklaw.com
Alexander Giza
Email: agiza@raklaw.com
Russ August & Kabat
12424 Wilshire Boulevard, 12th Floor
Los Angeles, CA 90025
310-826-7474
Fax: 310-826-6991

Hao Ni
Texas Bar No. 24047205
Ni Law Firm, PLLC
3102 Maple Ave. Suite 400
Dallas, TX 75201
Telephone: (214) 800-2208
Fax: (214) 880-2209
E-mail: hni@nilawfirm.com

Attorneys for Plaintiff
TQP Development, LLC